KASPERSKY LAB

Kaspersky Mobile Security 7.0 Enterprise Edition

USER'S GUIDE

KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION

User's Guide

© Kaspersky Lab
Tel/Fax: +7 (495) 797-8700, +7 (495) 645-7939,
+7 (495) 956-7000
http://www.kaspersky.com

Revision Date: July, 2008

Table of Contents

CHAPTER 1. KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION 5
1.1. Hardware and software requirements 6
1.2. Distribution Kit 6
1.3. Installing Kaspersky Mobile Security 6
1.3.1. Installing using the user's computer 7
1.3.2. Installing using an SMS message 7
1.4. Activating the application 8

CHAPTER 2. KASPERSKY MOBILE SECURITY FOR SYMBIAN OS 9
2.1. Using the application 9
2.1.1. Starting the application 9
2.1.2. Graphical user interface 10
2.1.3. General settings 11
2.1.4. Anti-virus scan and protection 12
2.1.5. Using Quarantine 19
2.1.6. Using Anti-Spam 21
2.1.7. Using Anti-Thief 26
2.1.8. Updating the application bases 29
2.1.9. Updating the application operation settings 33
2.1.10. Using the Firewall module 34
2.1.11. Viewing report about the application operation 35
2.2. Uninstalling the application 35

CHAPTER 3. KASPERSKY MOBILE SECURITY FOR MICROSOFT WINDOWS MOBILE 38
3.1. Getting started 38
3.1.1. Starting the application 38
3.1.2. Graphical user interface 39
3.2. Anti-virus scan and Real-Time protection 41
3.2.1. On-demand scan 41
3.2.2. Real-time protection 44
3.2.3. Scheduled scan 45

3.3. Using Quarantine ... 46
3.4. Using Anti-Spam and Anti-Theft modules ... 47
3.4.1. Anti-Spam module ... 47
3.4.2. The Anti-Theft tab ... 51
3.5. Updating the application bases ... 55
3.6. Updating the application operation settings ... 57
3.7. Firewall ... 57
3.8. Viewing reports about the application operation ... 58
3.9. Uninstalling the application ... 59

APPENDIX A. KASPERSKY LAB ... 64
A.1. Other Kaspersky Lab Products ... 65
A.2. Contact Us ... 75

APPENDIX B. LICENSE AGREEMENT ... 76

CHAPTER 1. KASPERSKY MOBILE SECURITY 7.0 ENTERPRISE EDITION

Kaspersky Mobile Security 7.0 Enterprise Edition is designed to ensure protection of mobile devices running Symbian OS and Microsoft Windows Mobile against malware programs and unsolicited e-mail messages and performs the following functions

- **Real-time protection** of the file system of the device - interception and scan of:
  - al incoming objects transmitted using wireless connections (IR port, Bluetooth) and EMS messages, during synchronization with the personal computer and downloading files using a browser;
  - files opened on the mobile device;
  - programs installed from the device's interface.
- **scanning of the file system's objects** on the mobile device or on the connected expansion cards by user's demand or according to the schedule;
- **reliable isolation of infected objects** in the quarantine storage;
- **updating of Kaspersky Mobile Security bases** used to scan for malware programs and delete dangerous objects.
- **blocking unwanted SMS messages**.
- **blocking access to or erasing user's data** in case of unauthorized actions with the device, as, for instance, theft.
- **protection of the mobile device at the network level**.

The user can use the capabilities providing flexible control of the Kaspersky Mobile Security operation settings, viewing the current anti-virus protection status and the event log in which the application's actions are recorded.

The application includes a menu system and support an easy-to-use user's interface.

Note

In case a detection of a malware program, Kaspersky Mobile Security can disinfect the infected object detected (if disinfection is possible), delete it or place it into the quarantine. In this case no copies of the object being deleted will be saved.

1.1. Hardware and software requirements

Kaspersky Mobile Security is designed for installation on mobile devices running one of the following operating systems:

- Symbian OS 9.1, 9.2 Series 60 UI.
- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

1.2. Distribution Kit

You can purchase Kaspersky Mobile Security via internet (the application distribution kit and documentation in the electronic form). Kaspersky Mobile Security can be also purchased in mobile communication offices. For more details contact you mobile communication operator.

1.3. Installing Kaspersky Mobile Security

The application is installed using a centralized installation using Kaspersky Administration Kit. The network Administrator can use one of the two methods of the application installation.

- installation using the user's computer;
- installation using an SMS message.

For more details about the remote installation of the application see Kaspersky Mobile Security 7.0 Enterprise Edition "Administrator's Guide".

1.3.1. Installing using the user's computer

After you connect the mobile device to a computer included into the Administration Server logical network, *kmlisten.exe* utility window will open (see Figure 1). This utility is designed to ensure installation of Kaspersky Mobile Security 7.0 Enterprise Edition onto a mobile device.

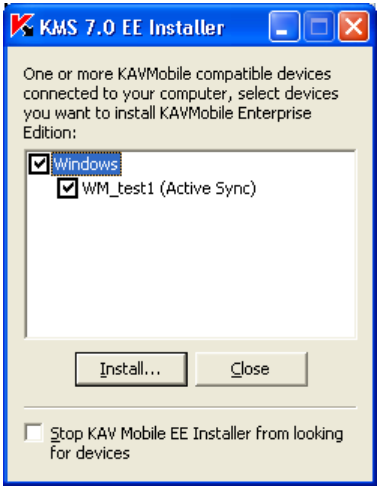
KMS 7.0 EE Installer
One or more KAVMobile compatible devices connected to your computer, select devices you want to install KAVMobile Enterprise Edition:
Windows
WM_test1 (Active Sync)
Install...
Close
Stop KAV Mobile EE Installer from looking for devices

Figure 1. **Kmlisten** utility

In order to install Kaspersky Mobile Security, perform the following actions:

using *kmlisten.exe* utility window, check the box next to the name of the device onto which you wish to install the application and press the **Install** button. The distribution kit for the application installation will be copied to your mobile device and started.

1.3.2. Installing using an SMS message

In order to install the application the network administrator can use the installation service using an SMS message (for details see Kaspersky Mobile Security 7.0 Enterprise Edition Administrator's Guide). An SMS message containing the URL of the server on which the application installation kit is located will be sent to the mobile device.

In order to install the application using an SMS message, perform the following actions:

1. Open an SMS containing URL of the server from which the Kaspersky Mobile Security installation package will be downloaded.
2. Use the link contained in the message text to download the application installation kit onto the device.
3. Save the application installation kit.

The application installation process will then start automatically.

1.4. Activating the application

Note

Activation of the application is required. Otherwise the application's functionality will not be available.

Activation of Kaspersky Mobile Security 7.0 Enterprise Edition is performed during synchronization with the Administration Server. During the synchronization the key file specified in the course of creating the policy for mobile devices (for more details about Kaspersky Administration Kit policies for mobile devices see Kaspersky Mobile Security 7.0 Enterprise Edition's Administrator's Guide).

The process of the application synchronization with the Administration service will be started automatically with the interval specified in the policy for mobile devices. You can also start the synchronization process manually (see section 2.1.9 on page 33 or on section 3.6 on page 57).

Note

While the policy is being created the possibility of mobile device key file modification must be blocked. Otherwise the device will not be activated during the synchronization with the Administration Server.

CHAPTER 2. KASPERSKY MOBILE SECURITY FOR SYMBIAN OS

This chapter contains description of the operation of Kaspersky Mobile Security 7.0 for devices running Symbian version 9.1, 9.2 or Series 60 UI operating system.

2.1. Using the application

This section contains information about configuration of the settings of the anti-virus scan and real-time protection, SMS message filtering, device anti-virus scan, bases update, application operation settings, device protection at the network level, etc.

2.1.1. Starting the application

In order to start Kaspersky Mobile Security, perform the following actions:

1. Open the device's main menu.
2. Select **KMS 7.0 EE** and start the application using the **Open** item from the **Options** menu.

After the device startup a window with main Kaspersky Mobile Security components (see Figure 2) will be displayed on the device screen.

- **Real-Time Protection** - using the real-time protection mode (see section 2.1.4 on page 12);
- **Last Full Scan** – date of the last anti-virus device scan.
- **Database date –** release date of the anti-virus database used by the application.
- **Anti-Spam Config.** – Anti-Spam operation mode (see section 2.1.6 on page 21).
- **Firewall level** – device protection level at the network level (see section 2.1.9 on page 33).

Figure 2. The Application component status window

In order to switch to the application interface, press **OK**.

2.1.2. Graphical user interface

The graphical user interface (GUI) contains six tabs:

- Using the **Scanner** tab you can perform an anti-virus can of the device, edit the anti-virus scan, real-time protection and quarantine settings and configure the auto scan schedule.
- Using the **Updater** tab you can update the anti-virus database, edit the updating settings and configure the updating schedule.
- Using the **Firewall** tab you can monitor the network activities and protect device at the network level.
- The **Anti-Theft** tab allows blocking the device and erase information from it in case the device gets lost or stolen (Anti-Theft module).
- Using the **Anti-Spam** tab you can configure filtering of incoming SMS messages (Anti-Spam module).
- Using the **Information** tab you can view application component's operation logs, general information about the application and the anti-virus bases used and edit general settings used for application's operation.

To navigate from one tab to another, use the joystick of the device or select the **Open Page** item in the **Options** menu (see Figure 3).

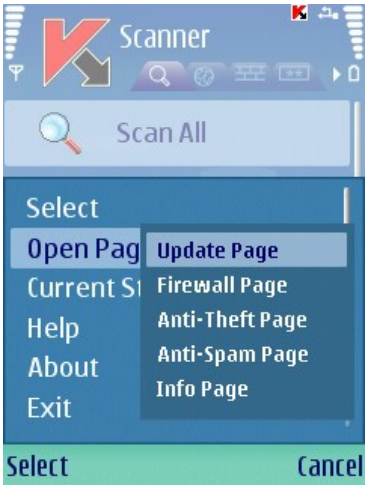

Figure 3. The **Options** menu

In order to return to the application components status window, select the **Current status** item in the **Options** menu.

2.1.3. General settings

Using settings in the **Information** tab in the **Settings** item (see Figure 4) you can configure the following application's functions:

- **Show Status Screen** determines whether the current status will be displayed at the application startup.
- **Log size** determines the maximum log size. Once the minimum value of the specified threshold has been reached, older messages in the log will be deleted until the maximum value of specified threshold is reached.
- **Screen Backlighting** determines whether the screen will be lit during the anti-virus scan. By default the backlight option is disabled.
- **Play Sound** controls the use of the sound notification in case of certain events (detection of an infected objects, message about an application status, etc.) By default the playback of the sound signal in case of a virus detection depends on the device profile (the setting's value **Profile**

dependent). Select **Enabled** if you wish to use the sound notification irrespective of the device profile selected.

- **Sound volume** determines the volume of the sound notification playback in case of the detection of an infected object.
- **Vibration** determines whether the device will vibrate when an infected object is detected. By default vibration is enabled.

Figure 4. The **Settings** menu

In order to edit the values of the settings, use the device's joystick or select the **Change** item in the **Options** menu.

2.1.4. Anti-virus scan and protection

Using the **Scanner** tab you can perform anti-virus scan of the entire file system and the memory of the device or of an individual folder or file. You can also modify the settings of the anti-virus scan and of the real-time anti-virus protection, view the report about the scan results and create the automatic scan start schedule.

2.1.4.1. Real-time protection and on-demand scan

Real-time protection is the mode of operation in which the resident part of Kaspersky Mobile Security is constantly loaded in the device's RAM and monitors all data including the incoming data received by the device.

Real-time protection is started since the moment the device is turned on and works until it is turned off (if the use of this mode was not disabled by the protection settings).

Kaspersky Mobile Security also allows to perform a full scan of the device's file system including the analysis of objects located on the connected memory expansion cards.

Information about the results of the Real-time protection and of the on-demand scan will be recorded in the report. In order to view the report, select the **Reports** item in the **Scanner** tab.

To start Real-Time protection, do the following:

1. Select the **Settings** item in the **Scanner** tab.
2. Select the **Monitor Settings** in the **Settings** section.
3. Enable / disable Real-Time protection by setting the **Real-time protection** setting certain value to a corresponding value.

To modify the Real-Time protection operation settings, do the following:

1. Select the **Settings** item in the **Scanner** tab.
2. Select the **Monitor Settings** in the **Settings** section.
3. Define the scan area in the **Scan Mask** block by selecting the file types to be scanned:
   - **All files** – scan all files.
   - **Executable files** – scan only executable program files (for example *.exe, *.sis, *.mdl, *.app).
4. Determine the action to be performed when an infected object has been detected (the **Virus Found Fction** setting).

   By default detected malware objects are placed into quarantine (the **Quarantine** setting value).

   To ensure that information about detection of an infected object is logged in the application’s report, select value **Log event**.

To make the application delete detected malware objects without prompting user for action, select the **Auto Delete** value.

5. Enable / disable new card scan mode (the **Scan New Card** setting).

   By default, if a memory card is detected, the application notifies that the card must be scanned.

   To enable the scan of flash-cards, connected to the device, set the **Auto Scan** value. In order to disable the automatic scan of flash cards, select **Disable**.

6. Enable / disable the display of the protection icon (the **Show Monitor icon** setting).

   Select the **Always** value in the corresponding item of the menu if you wish the application icon to be always displayed on the device's screen when the real-time protection is enabled. If you wish the icon to be displayed only in the device's menu, select **Only in menu**. If you do not wish this icon to be displayed, select **Off**.

To modify the on-demand scan operation settings, do the following:

1. Select the **Settings** item in the **Scanner** tab.
2. Select the **Scan Settings** in the **Settings** section.
3. Define the scan area in the **Scan Mask** block by selecting the file types to be scanned:
   - **All files** – scan all files.
   - **Executable files** – scan only executable program files (for example *.exe, *.sis, *.mdl, *.app).
4. Determine the action to be performed when an infected object has been detected (the **Virus Found Action** setting).

   By default the application attempts to disinfect detected malware objects (the setting value **Try to disinfect**).

   To place detected malware objects into quarantine, select the **Quarantine** value.

   To ensure that information about detection of an infected object is logged in the application’s report, select value **Log event**.

   To make the application delete detected malware objects without prompting user for action, select the **Auto Delete** value.

   To ensure that a notification with a prompt for action is opened once an infected object is detected, select the **Ask User** value.

5. Specify an action to be performed if disinfection of an infected object is impossible (**If disinfection fails** setting).

   By default detected malware objects are placed into quarantine (the **Quarantine** setting value).

   To ensure that information about detection of an infected object is logged in the application's report, select value **Log event**.

   To make the application delete detected malware objects without prompting user for action, select the **Auto Delete** value.

   To ensure that a notification with a prompt for action is opened once an infected object is detected, select the **Ask User** value.

6. Enable / disable the scan of the device ROM memory (the **Scan ROM** setting).

   In some situations the ROM memory may become vulnerable for malware programs. To enable ROM memory scan, select the **Yes** value.

7. Enable / disable unpacking of SIS and ZIP archives (the **Unpack archives** setting).

   If you wish the application unpack SIS and ZIP archives, select **Yes**. If archives do not need to be unpacked during the scan, select **No**.

Note

In order to edit the values of the settings, use the device's joystick or select the **Change** item in the **Options** menu.

By default the application uses the values of the settings recommended by Kaspersky Lab's specialists. If you wish to return to the recommended values of the settings while you are using the application, open the **Scanner** tab and select the **Set Default** item from the **Options** menu.

In order to start an anti-virus scan, perform the following actions:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Using the **Scanner** tab (see Figure 5) select the **Scan All** item if you wish to scan the entire file system of the device or **Scan Folder** if you wish to scan an individual folder.

Figure 5. The **Scan** tab

When **Scan Folder** item is selected, a window displaying the device's file system will open. In order navigate through the file system use the joystick buttons of your device. In order to scan a folder, move the cursor to the folder you wish to scan and select the **Start Scanning** item from the **Options** menu.

After the scan is started, the scan process window will open in which the current status of the task will be displayed: the number of scanned objects, the path to the object being scanned at the time and the percentage indicator of the progress (see Figure 6).

Figure 6. The **Scan progress** window

Once an infected object is detected the action specified by the corresponding setting in the **Settings→Scan Settings** section will be performed.

Figure 7. Notification about virus detection

Once the scan is complete the general statistics about detected and deleted malware objects will be displayed.

To disable screen backlight during the scan,

switch to the **Information** tab, open the **Settings** menu and select the **Yes** value for the **Screen Backlighting** setting.

By default the backlight will go off automatically to save the battery charge.

2.1.4.2. Scheduled scan

Kaspersky Mobile Security allows the user to create the schedule for the automatic device scan. The scan is performed in the background mode. When detecting an infected object an action specified in the scan settings will be performed with such object (see section 2.1.4.1 on page 13).

By default scheduled scan is disabled.

Figure 8. The **Schedule** menu

To create the scan launch schedule:

select the **Schedule** item in in the Scan tab and specify the **Auto Scan** settings (see Figure 8):

- **Daily** - the scan to be performed every day. Specify the **Auto Scan Time** in the entry field.
- **Weekly** - the scan will be performed once a week. Specify the **Auto Scan Day** and **Auto Scan Time**.

2.1.5. Using Quarantine

Infected objects placed into the quarantine do not impose any threat for the device and can be deleted or restored later.

Detected infected objects can be quarantined by the application automatically or after your confirmation.

If you wish the application to place detected malware objects into the quarantine without the prompt, do the following:

1. Open the **Scanner** tab.
2. Select the **Settings** item.
3. Select the **Scan Settings** or the **Monitor Settings** item.
4. Select **Quarantine** as the value for the **Virus Foud Action** setting.

If you selected **Ask User** as the action to be performed, then, when an infected object is detected, Kaspersky Mobile Security will offer that you either delete this object or quarantine it.

To view the list of quarantined objects,

open the **Scanner** tab and select the **Quarantine** item (see Figure 9).

Figure 9. Infected quarantined objects

The **Options** menu accessible from the quarantine view window allows the user:

- To view detailed information about each object in the quarantine (**View details**).
- Delete the selected object (**Remove file**).
- Clear the quarantine by deleting all quarantined objects (**Remove all**).
- Restore the selected object from the Quarantine to its original folder (**Restore file**).
- **V**iew Quarantine Help (**Help**).

In order to set the quarantine settings:

1. Open the **Scanner** tab.
2. Select the **Settings** item.
3. Select the **Quarantine** tab (see Figure 10).

Figure 10. Quarantine settings

The **Quarantine size** setting determines the maximum number of infected objects which can be stored in the quarantined. The possible values are **20**, **50** or **100** files.

The **Store Limit** setting determines the period of time during which the infected objects can be stored in the quarantine. After this period elapses, the infected objects will be automatically deleted.

Note

In order to restore the values of the quarantine settings recommended by Kaspersky Lab's specialists select **Set Default** from the **Options** menu.

2.1.6. Using Anti-Spam

The Anti-Spam module is designed to ensure protection of your device against unsolicited SMS messages.

Filtering is based on the use of "black" and "white" lists. These lists contain phone and sample phrases characteristic of spam and non-spam messages. Message analysis will be performed in the following order:

- check if the sender's number is included into the "black" list;
- check if the sender's number is included into the "white" list;
- scan of the message text for the presence of phrases found in the "black" list;
- scan of the message text for the presence of phrases found in the "black" list;

If at least one match is detected, the scan will be stopped. The message containing an element found in the "black" list will be blocked. The message containing an element found in the "white" list will be passed.

2.1.6.1. Anti-Spam work modes

Anti-Spam filters messages in one of the following modes:

- **Enabled.** In this mode Anti-Spam filters incoming messages using the "black" and the "white" lists. Once a message is received from a phone number not found in either of the lists, Anti-Spam will notify the user and will offer to block or allow receipt of the message and to add this phone number to the "white" or "black" list.
- **Black list.** In this mode Anti-Spam blocks receipt of messages matching the "black list" criteria. All other messages will be passed.
- **White list.** In this mode Anti-Spam passes messages matching the "white list" criteria. All other messages will be blocked.
- **Disabled.** In this mode Anti-Spam is disabled. No filtering of incoming messages is provided.

To select the Anti-Spam operation mode:

1. Open the **Anti-Spam** tab.
2. Select the **Settings** item.
3. Set the operation mode using the **Config. Anti-Spam** setting.

2.1.6.2. Editing “black” and “white” lists

"Black" and **"White"** lists contain records with phone numbers, SMS from which will be block or passed by Anti-Spam. Information about blocked or deleted messages will be entered in the **Log** section.

> **Note**
>
> Messages not included into either list will not blocked!

To enter changes into the "black" or "white" list,

open the **Anti-Spam** tab and select the corresponding item (see Figure 11).

To edit the list use the **Options** menu:

- **Add Record** – add a new record to the list.
- **Edit Record** – edit the current record.
- **Remove Record** – delete entry from the list.
- **Remove All** – clear the list by deleting all records.
- **Help** – view Help on managing the list.

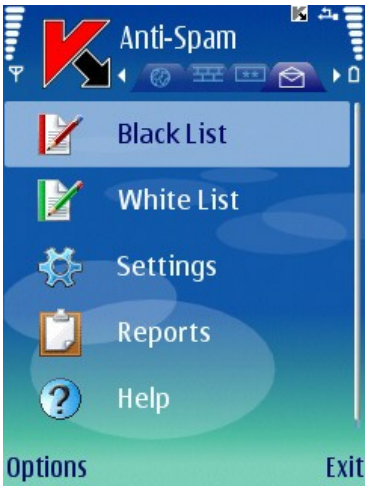

Figure 11. The **Anti-Spam** tab

- When you select the **Add Record** or the **Edit Record** item, you will be offered to specify the following record's parameters (see Figure 12)
- **Phone number**. Specify the phone number for which receipt of messages will be blocked or allowed. Such number may begin with a digit or with a "+" and must contain digits only. Additionally when specifying a number, you can use masks "?" and "*".
- **Text**. Specify the text upon detection of which in the message received, such message will either be passed or blocked.

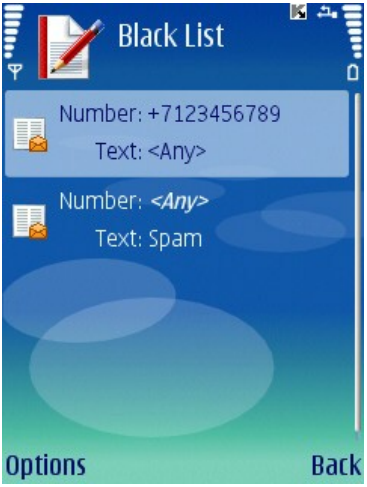

Figure 12. The Black List

2.1.6.3. Anti-Spam operation settings

To edit Anti-Spam settings:

open the **Anti-Spam** tab and select the **Settings** item (see Figure 13).

Figure 13. Anti-Spam settings

The following Anti-Spam settings are accessible in the **Settings** menu:

- **Config. Anti-Spam** – Anti-Spam operation mode (see section 2.1.6.1 on page 21).
- **Allow Contacts List**. If the setting is assigned value **Yes**, Anti-Spam will not block receipt of messages from numbers contained in your phone book. If this option is disabled (**No** value), Anti-Spam will perform filtering depending on whether the phone number is included into the "white" or "black" list.
- **Add outgoing**. If the setting is assigned value **Yes**, all phone numbers to which you send SMS messages will be automatically added to the "white" list. To disable this option, select **No**.
- **Block non-numeric.** If this setting is assigned value **No**, Anti-Spam will not block all incoming messages from non-numeric numbers. To enable this option, select **Yes**.

> **Note**
>
> This setting affect only records created by Anti-Spam in one of the following situations:
>
> - adding outgoing numbers to the "white" list (setting **Add outgoing** is enabled);
> - adding new phone numbers from which messages are received to one of the lists (see section 2.1.6.4 on page 25).

In order to edit the values of the settings, use the device's joystick or select the **Change** item in the **Options** menu.

2.1.6.4. Actions to be performed with messages

When you receive an SMS or an MMS message from a phone number not found in either the "black" or the "white" list, such message will be intercepted by Anti-Spam and a notification will be displayed on the screen of the device (see Figure 14xxx)

Using the **Options** menu you can select one of the following actions to be performed with the message:

- **Add to White List** – allow receipt of messages and add the sender's phone number to the "white" list.
- **Add to Black List** – block messages and add the sender's phone number to the "black" list.

- **Skip** – allow the receipt of the message. In this case the sender's phone number will not be added to either of the lists.

Information about blocked messages will be entered into the application log. In order to view the report, select the **Reports** item in the **Anti-Spam** tab.

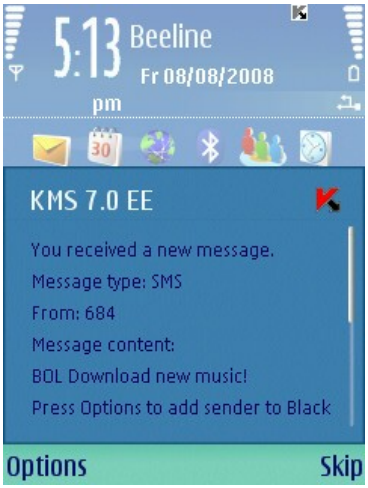

Figure 14. Anti-Spam warning

2.1.7. Using Anti-Thief

The Anti-Thief module is designed to ensure protection of data stored on the mobile device against unauthorized access to it in case the device was list or stolen.

When you access the module settings for the first time you will have to set up a password. Later this password is used to obtain access to the module's settings and managing its functions. **SMS-Block** function – allows blocking the device at the user's discretion. You can unblock the device only after you enter a password used to access the Anti-Theft module. To unblock the device using the SMS-Block function, send an SMS message containing text: "`block:code`" to the device. By default the SMS-Block function is disabled. To enable the function select **On**.

The **SMS-Clean** allows erasing user's personal data (contacts, messages, files, data from the memory card, network settings). To use the SMS-Clean function, and an SMS containing text "clean:code" to the device. By default the SMS-Clean function is disabled. To enable the function select **On**.

SIM Watch – allows to send to the specified numbers a new phone number and to block the stolen device if the SIM card was replaced in such stolen device. To enable the function select **On**.

If it is necessary to change the password used to work with Anti-Theft module, select the **Change password** item. Enter the new password and its confirmation and press the **OK** button.

Each time when you access the Anti-Theft module settings (see Figure 14) you have to enter the password you have set up earlier.

Figure 15. The **Anti-Theft** tab

Information about the module's work will be entered into the application log. In order to view the report, select the **Reports** item in the **Anti-Theft** tab.

2.1.7.1. Section SMS-Clean

To configure the SMS-Clean function operation settings:

1. Open the **Anti-Theft** tab and enter the password (see section 2.1.7 on page 26).
2. Select the **Settings** item.
3. Select the **SMS-Clean** item.

Section **SMS-Clean** contains the list of data which can be selected for deletion if your device gets lost (see Figure 16).

Figure 16. The **SMS-Clean** tab

If you wish to be able to delete the phone book once your mobile device has been stolen or lost, select the **Remove contacts** item and assign value **Yes** to it.

Note

Contacts will be erased only from the phone book stored in the device. SIM card phone book will not be deleted.

In order to delete mail, SMS messages (Inbox and Mailbox folders) select the **Clean inbox** and assign value **Yes** to it.

The **Remove personal files** item ensures deletion of personal data (data from folder !:\Data\). By default deletion of personal files is not provided. If you wish to be able to delete your personal data in case your device is stolen or lost, select this item and assign value **Yes** to it.

Use the **Remove card files** item to enable clearing the memory card on the lost device. By default this ability is disabled. To enable erasing of data from the memory card, select the **Remove card files** and select the **Yes** value.

To enable the option of deleting network connection settings, select the **Delete network settings** item and set the value to **Yes**.

Press **OK** to save the changes.

2.1.7.2. SIM Watch settings

To configure the SIM Watch settings, switch to the **Anti-Theft** tab. Enter the password (see section 2.1.7 on page 26) and then select **SIM Watch** in the window that will open.

Section **SIM Watch** is designed to monitor replacement of the SIM card in the device (see Figure 17).

Figure 17. The **SIM Watch** tab

Using fields **Phone number 1** and **Phone number 2** enter phone numbers to which you would like to receive a new phone number if the SIM card was replaced in your device. Such numbers may begin with a digit or with a "+" and must contain digits only.

Also you can enable blocking your device if the SIM card was replaced. To do it, select the **Block device** item and assign value **Yes** to it. You can unblock the device by entering the password set up to access the Anti-Theft module. By default blocking of the device is not provided.

Press the **OK** button to save the changes you have made.

2.1.8. Updating the application bases

Scan for malware programs is performed based on the records in the application's bases which contain description of all malware programs known at the moment. It is extremely important to keep you bases up-to-date.

You can update bases manually or according to a schedule. Updates are performed from Kaspersky Lab's servers via internet.

You can enable automatic anti-virus scan of your device after each update of the Kaspersky Mobile Security bases. In order to do it, switch to **Settings** item in the **Updater** tab and assign value **On** to the **Scan on Update** item.

The value of the **Scan Quar. on Update** setting determines whether or not objects in the quarantine will be rescanned each time after the application bases have been updated. By default the scan is performed. If you do not wish the scan to be performed, select **Off**.

If it is necessary to change the active access point, use the **Access point** setting. Then select the require value in the list. By default the access point is the default point of the device.

The value of the **Update server** setting determines the application bases update source: Kaspersky Lab's update servers (**Use default** value) or another server specified by the user (**User defined** value). If you selected the **User defined** value, enter the URL in the window that will open. If required, you can specify an alternative update server.

You can view detailed information about bases used in the **Database Info** item in the **Information** tab.

Information about bases update will be entered into the log. In order to view the log, select the **Reports** item in the **Updater** tab.

2.1.8.1. Updating settings

In order to configure application bases updates, perform the following actions:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Switch to the **Settings** item in the **Updater** tab (see Figure 18).

Figure 18. The **Updater** Tab

3. Select the access point (the **Access Point** setting) (see Figure 19).

> **Note**
>
> The access point is configured using settings provided by your wireless service provider.

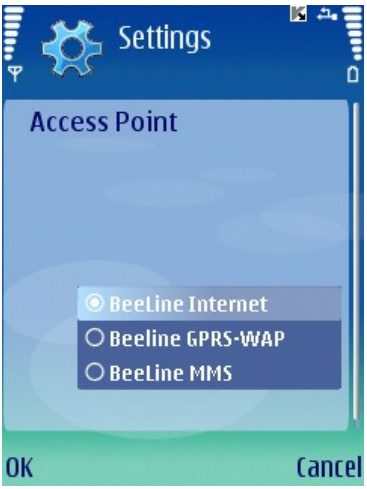

Figure 19. Selecting the access point

4. Enter the address of the update server (if necessary). In order to do it, select the **Update server** item and then select the **User defined** value. Enter the URL of the update source in the window that will open (see Figure 20).

Figure 20. Update server address

By default updates are performed from Kaspersky Lab's update server: http://ftp.kaspersky.com/index/mobile.xml.

Note!

Irrespective of whether the connection was opened earlier, it will be closed after the update is complete.

2.1.8.2. Manual update

To start a manual update of Anti-Virus databases:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Select the **Update** item in the **Updater** tab (see Figure 18)

2.1.8.3. Scheduled update

To create an application bases update launch schedule.

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).

2. Select the **Schedule** item in the **Updater** tab and configure the **Auto Update** settings:

   - **Off** – to not perform scheduled updates.
   - **Daily** - the update to be performed every day. Specify the update time in the corresponding field.
   - **Weekly** - the update will be performed once a week. Specify the update date and time in the corresponding fields.

2.1.9. Updating the application operation settings

Note

For details about the joint operation of Kaspersky Mobile Security and Kaspersky Administration Kit see Kaspersky Mobile Security Administrator's Guide.

While using Kaspersky Mobile Security jointly with Kaspersky Administration Kit the application operation settings will be set by the policy for a group of mobile devices. Activation of the application and the applying of the policy settings blocked to prevent changes will take place when a device is being added to the administration group.

Later synchronization of the application with the Administration Server will be performed automatically using intervals set in the policy settings.

In order to start application manual synchronization with the Administration Server:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Open the **Updater** tab.
3. Select **Synchronization** item.

During the synchronization the application operation settings will be loaded from the Administration Server and reports about the application's operation will be sent from the device to the application server. If the application operation settings did not change since the time of the last synchronization, the policy settings will not be applied.

2.1.10. Using the Firewall module

Firewall module is designed for monitoring the network activity and protection of your mobile device at the network level (see Figure 21).

You can select the protection level (**Firewall** setting) in order to specify the level of control over the incoming and outgoing traffic out of the suggested options:

- **High** – any network activity except updating of bases and connection to Kaspersky Administration Kit is blocked.
- **Medium** – all incoming connections will be blocked, outgoing connections can only be established using SSH, HTTP, HTTPS, IMAP, SMTP ports.
- **Low level** – only incoming connections will be blocked.
- **Off** – all network activities will be allowed.

Using the **Notifications** setting you can enable/disable the user's notification about an attempt to establish a connection blocked at the Firewall protection level selected. In order to disable receipt of notifications, select **Off**.

Figure 21. The **Firewall** tab

Information about the Firewall module's work will be entered into the application log. In order to view the report, select the **Reports** item in the **Firewall** tab.

2.1.11. Viewing report about the application operation

You can view the chronological event log about the operation of Kaspersky Mobile Security in the **Information** tab. In order to do it switch to this tab and select the **Reports** item (see Figure 22).

Figure 22. Report about the application's work

2.2. Uninstalling the application

In order to uninstall Kaspersky Mobile Security, perform the following actions:

1. Close Kaspersky Mobile Security. To do this:
   a) Press and hold the **Menu** button.
   b) Select **KMS 7.0 EE** in the list of the running applications and press the **Options** button.
   c) Select the **Close** menu item (see Figure 23).

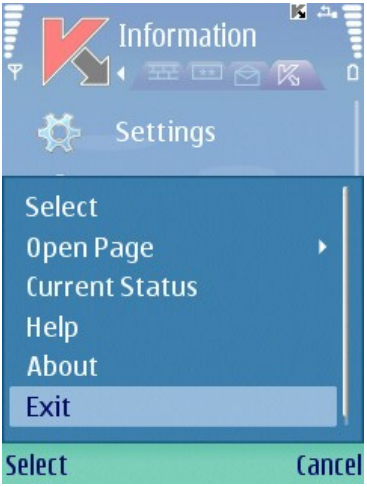

Figure 23. Closing the application

2. Uninstall Kaspersky Mobile Security

   a) Press the **Menu** button and select the **Application Manager** menu item (see Figure 24).

Figure 24. Starting the **Application Manager**

   b) Select **KMS7.0 EE** in the list of applications and press the **Options** button (see Figure 25).

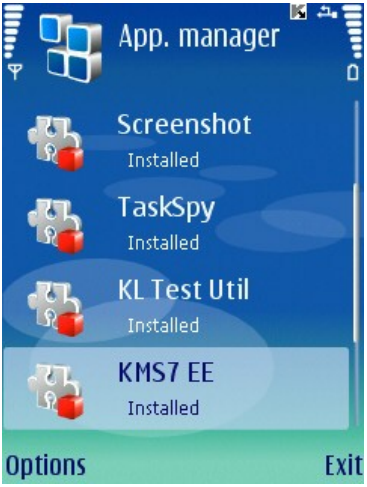

Figure 25. Selecting the application

c) Select the **Remove** menu item (see Figure 26).

Figure 26. Uninstalling the application

d) Press the **Yes** button in the prompt to confirm the application removal.

CHAPTER 3. KASPERSKY MOBILE SECURITY FOR MICROSOFT WINDOWS MOBILE

This chapter contains description of the operation of Kaspersky Mobile Security for mobile devices running one of the following operating systems:

- Microsoft Windows Mobile 5.0.
- Microsoft Windows Mobile 6.0.

3.1. Getting started

This section contains information on how to start the application. It also contains information about the general principles of the graphic user's interface.

3.1.1. Starting the application

In order to start Kaspersky Mobile Security, perform the following actions:

1. Open the **Programs** menu on your mobile device.
2. Select **KMS 7.0 EE** in order to start the application.

After the application startup a window with main Kaspersky Mobile Security components (see Figure 27) will be displayed on your mobile device's screen.

- **Real-Time protection** – the use of the Real-Time protection mode.
- **Last scanned** – date of the last anti-virus scan of your mobile device.
- **Last updated –** release date of Kaspersky Mobile Security database used by the application.

> **Note!**
>
> If anti-virus scan of your mobile device has never been performed or if it two weeks or more have passed since the last update of the anti-virus database, the icon next to the corresponding item will look as follows: ⚠. This icon will also appear if the real-time protection mode or the Anti-Spam modules is disabled.

- **Firewall** – device protection level at the network level.
- **Anti-Spam** – the status of the Anti-Spam module used for filtering SMS messages.

> **Note!**
>
> Anti-Spam module is not provided for PDAs!

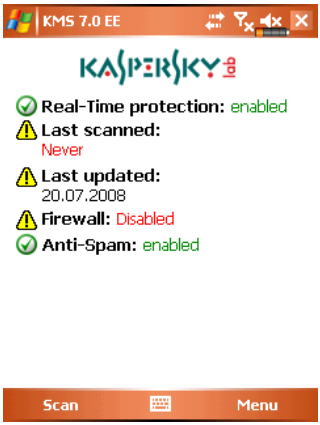

Figure 27. The Application component status window

3.1.2. Graphical user interface

The graphical user's interface consists of six tabs access to which is provided via **Menu** (see Figure 28):

- Using the **Scan** tab you can perform an anti-virus can of the mobile device, edit the anti-virus scan, real-time protection and quarantine settings and create the auto scan schedule (see section 3.2 on page 41).

- Using the **Firewall** section you can monitor the network activities and protect the device at the network level (see section 3.7 on page 57).
- Using the **Update** section you can update the anti-virus database, edit the updating settings and configure the updating schedule (see section 3.5 on page 55).
- Using the **Anti-Spam** section you can configure filtering of incoming SMS messages (Anti-Spam module) (see section 3.4.1 on page 47).
- Using the **Anti-Theft** section you can block the device and erase information stored on it in case it gets lost or stolen (the Anti-Theft module) (see section 3.4.2 on page 51).
- Using the **Information** section you can view application components' operation logs, general information about the application and bases being used (see section 3.8 on page 58).

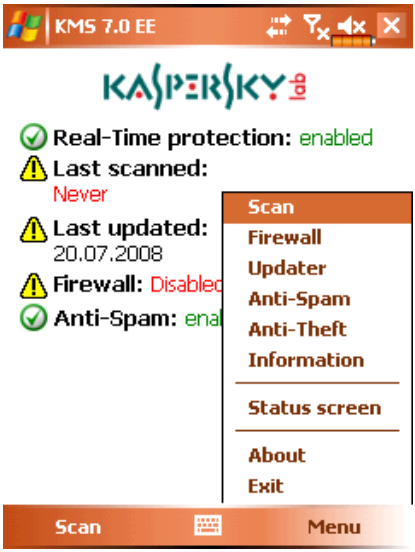

Figure 28. The application menu

In order to return to the application components status window, select the **Status screen** item.

To view the general information about the application, select the **About** item.

To close the application, select **Exit**.

3.2. Anti-virus scan and Real-Time protection

Using the **Scan** section you can perform anti-virus scan of the entire file system and the memory of the mobile device or of an individual folder or file. You can also modify the settings of the anti-virus scan and of the real-time anti-virus protection, view the report about the scan results and create the automatic scan start schedule.

3.2.1. On-demand scan

To modify the on-demand scan settings, do the following:

1. Select the **Scanner Settings** in the **Scan** section.
2. Define the scan area in the **Scan options** block by selecting the file types to be scanned:
   - **Scan archives** - scan files packed into archives.
   - **Executables only** - scan only executable program files.
3. In the **If a virus is detected** block, determine the action to be performed by the application once an infected object is found. If disinfection is not required, select the possible anti-virus action by selecting one of the following values for the **Primary action** setting:
   - **Quarantine** – move infected objects detected to the quarantine.
   - **Ask user** - display a message about a virus detection on the screen with a suggestion to delete, quarantine or skip the infected object.
   - **Delete** - delete infected objects detected.
   - **Skip** – do not perform any action with the infected objects.

   If you want the application to attempt to disinfect a detected infected object, check the **Try to disinfect** box. Select an action to be performed by the application if disinfection is impossible in section **If disinfection fails**.

In order to start an anti-virus scan, perform the following actions:

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 38).

2. Using the **Scan** section (see Figure 29) select the **Scan Phone** item if you wish to scan the entire file system of the mobile device or **Scan Folder** if you wish to scan an individual folder.

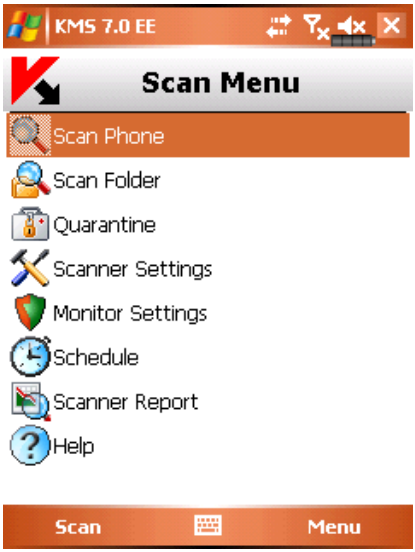

Figure 29. The **Scan** section

When **Scan Folder** item is selected, a window displaying the mobile device's file system will open. In order to start the scan of a folder, move the cursor to the folder and press the **Scan** button.

After the scan is started, the scan process window will open in which the current status of the task will be displayed: the number of objects scanned and the path to the object currently being scanned (see Figure 30).

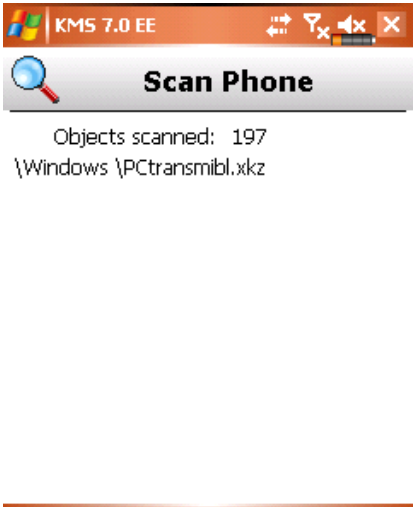

Figure 30. The **Scan progress** window

Figure 31. Notification about virus detection

Once the scan is complete the general statistics about detected and deleted malware objects will be displayed.

3.2.2. Real-time protection

Real-time protection is the mode of operation in which the resident part of Kaspersky Mobile Security is constantly loaded in the mobile device's RAM and scans executable program files and files being opened by the user.

Real-time protection is started since the moment the device is turned on and works until it is turned off (if the use of this mode was not disabled during configuration of the protection settings).

Additionally, Kaspersky Mobile Security allows to perform a full scan of the mobile device's file system.

Information about the results of the Real-time protection and of the on-demand scan will be recorded in the report. To view the report, select the **Scanner report** item. The report is also available in the **Information** section (see section 3.8 on page 58);

To enable Real-Time protection, do the following:

1. Select the **Monitor Settings** in the **Scan** section.
2. Check the **Enable Real-Time Prot.** box.

To modify the Real-Time protection operation settings, do the following:

1. Select the **Monitor Settings** in the **Scan** section.
2. Check the **Executables only** box in the **Scan options** section if you wish Real-Time protection to scan only executable program files. Uncheck the box to make Real-Time Protection to scan executable program files and files being opened by the user.
3. In the **If a virus is detected** block, select the action to be performed by the application once an infected object is found. You can select one of the following options:
   - **Quarantine** – move infected objects detected to the quarantine.
   - **Delete** - delete infected objects detected.
   - **Skip** – do not perform any action with the infected objects.

3.2.3. Scheduled scan

Kaspersky Mobile Security allows the user to create the schedule for the automatic scan of the mobile device. The scan is performed in the background mode. When detecting an infected object an action specified in the scan settings will be performed with such object (the **Scanner settings** item).

By default scheduled scan is disabled.

In order to create a schedule for launching a device's file system:

select the **Schedule** item in the **Scan** section and create a scan launch schedule (see Figure 32):

- **Daily** - the scan to be performed every day. The scan time is determined by the **Time** setting.
- **Weekly** - the scan will be performed once a week. The date and time of the scan will be determined by settings **Day of week** and **Time**.
- **Manual** - the update will be manually launched by the user.

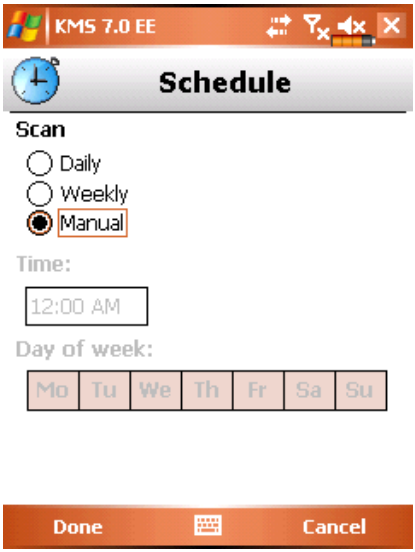

Figure 32. The **Schedule** menu

3.3. Using Quarantine

Infected objects placed into the quarantine do not impose any threat for the mobile device and can be deleted or restored later.

Detected infected objects can be quarantined by the application automatically or after your confirmation.

In order to enable automatic movement of infected objects to the quarantine:

1. Open the **Scan** section,
2. Select the **Scanner Settings** item.
3. In the **If a virus is detected** section select **Quarantine** as the action to be performed in case of a detection of a malware object.

   If you select **Ask user** as the action to be performed, then, once an infected object is detected, a notification window containing a prompt to either delete the object or quarantine it.

In order to view quarantine content,

open the **Scan** section and select the **Quarantine** item (see Figure 33).

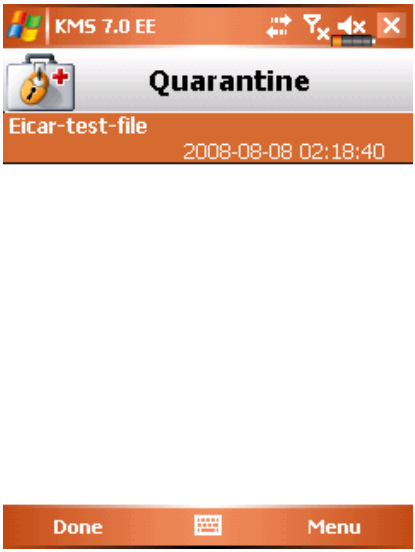

Figure 33. **Quarantine**

The **Menu** accessible from the quarantine view window allows the user:

- To view detailed information about the selected object in the quarantine (**Detailed info** item).
- Delete the selected object (**Delete File** item).
- Restore the current object from the Quarantine to its original folder (**Restore** item).
- Clear the quarantine by deleting all quarantined objects (**Empty quarantine** item).

3.4. Using Anti-Spam and Anti-Theft modules

The Anti-Spam module is designed to ensure protection of your device against unsolicited SMS messages.

Filtering is based on the use of "black" and "white" lists. These lists contain phone and sample phrases characteristic of spam and non-spam messages. Message analysis will be performed in the following order:

- check if the sender's number is included into the "black" list;
- check if the sender's number is included into the "white" list;
- scan of the message text for the presence of phrases found in the "black" list;
- scan of the message text for the presence of phrases found in the "black" list;

If at least one match is detected, the scan will be stopped. The message containing an element found in the "black" list will be blocked. The message containing an element found in the "white" list will be passed.

3.4.1. Anti-Spam module

The Anti-Spam module is designed to ensure protection of your mobile against unsolicited SMS messages.

Note!

Anti-Spam module is not provided for PDAs!

Filtering is based on the use of "black" and "white" lists. These lists contain phone and sample phrases characteristic of spam and non-spam messages. Message analysis will be performed in the following order:

- check if the sender's number is included into the "black" list;
- check if the sender's number is included into the "white" list;
- scan of the message text for the presence of phrases found in the "black" list;
- scan of the message text for the presence of phrases found in the "black" list;

If at least one match is detected, the scan will be stopped. The message containing an element found in the "black" list will be blocked. The message containing an element found in the "white" list will be passed.

To edit Anti-Spam settings do the following:

1. Select **Settings** in the **Anti-Spam** section.
2. Select the operation mode using the **Anti-Spam** using the **Anti-Spam** setting:
   - **Normal.** In this mode Anti-Spam filters incoming messages using the "black" and the "white" lists. Once a message is received from a phone number not found in either of the lists, Anti-Spam will notify the user and will offer to block or allow receipt of the message and to add this phone number to the "white" or "black" list.
   - **"Black" list only.** In this mode Anti-Spam blocks receipt of messages matching the "black list" criteria. All other messages will be passed.
   - **"White" list only.** In this mode Anti-Spam passes messages matching the "white list" criteria. All other messages will be blocked.
   - **Disabled.** In this mode Anti-Spam is disabled. No filtering of incoming messages is provided.
3. Check the **Allow contacts** box so that Anti-Spam would not block receipt of messages from numbers found in the contact list.
4. Check the **Block non-numeric** box so that Anti-Spam would block receipt of messages from non-numeric numbers.

3.4.1.1. Editing "black" and "white" lists

The "Black" list contains entries which, if found in messages, makes Anti-Spam block such messages.

The “Black” list contains entries, which, if found in messages, makes Anti-Spam block such messages.

To edit the "black" or "white" list,

open the **Anti-Spam** section (see Figure 34) and select the corresponding list.

To edit the list use the **Menu**:

- **Insert number** – add a new record to the list.
- **Delete number** – delete record from the list.
- **Edit number** – edit the current record in the list.

Select the **Insert number** item and specify your phone number (field **Enter phone**) you wish to be included into the list. This number may begin with a digit or with a "+". Additionally when specifying a number, you can use masks "?" and "*".

You can also specify the text (**Enter text** field) upon the detection of which in a message the following actions will be performed:

- the message in which such text specified for the "white" list is found will be allowed to pass;
- the message in which such text specified for the "black" list is found will be blocked;

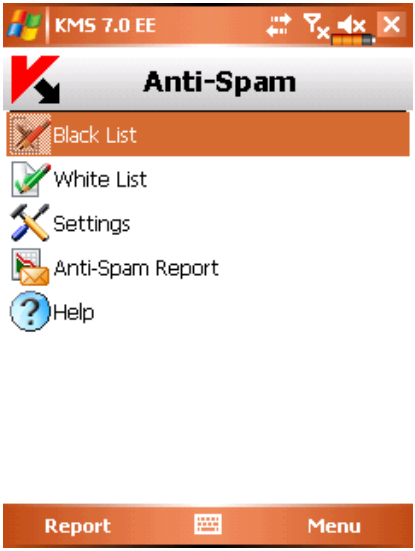

Figure 34. The **Anti-Spam** section

After you are done editing the list, press **Done** to return to the **Anti-Spam** section.

3.4.1.2. Actions to be performed with messages

When you receive messages from a phone number not found in the "black" or "white" list depending that the Anti-Spam settings allow the receipt of message from unknown numbers (see section 3.4.1 on page 47), a warning will be displayed on the mobile device's screen (see Figure 35).

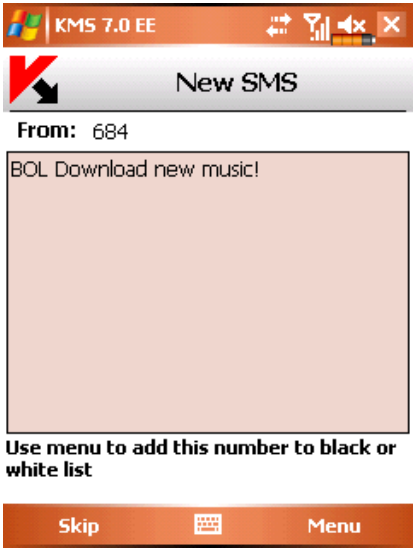

Figure 35. Anti-Spam warning

Using the **Menu** you can select one of the following actions to be performed with the message:

- **Add to WhiteList** – allow receipt of messages and add the sender's phone number to the "white" list.
- **Add to BlackList** – block messages and add the sender's phone number to the "black" list.

Press the **Pass** button in order to let the message pass. In this case the sender's phone number will not be added to either of the lists.

Information about blocked messages will be entered into the application log.

In order to view the log, select the **Anti-Spam Report** item in the **Anti-Spam** section. The report is also available in the **Information** section (see section 3.8 on page 58);

3.4.2. The Anti-Theft tab

The Anti-Thief module (section **Anti-Theft** (see Figure 36) is designed to ensure protection of data stored on the mobile device against unauthorized access to it in case the device was list or stolen.

When you access the module settings for the first time you will have to set up a password. Using this password you can obtain access to the module's settings and activate the module functions. The password is required in order to prevent unauthorized access to the module operation settings and to enable the user to block and erase information saved on the device in case it is stolen or lost.

SMS-Block function – allows blocking the device at the user's discretion. You can unblock the device only after you enter a password used to access the Anti-Theft module. The action of this function gets triggered after the user sends an SMS message “block:code” to the device that got lost.

SMS-Clean allows erasing user's personal information (contact, incoming messages, personal files, network connection settings). The action of this function gets triggered after the user sends an SMS message “clean:code” to the device that got lost.

The **SIM Watch** allows sending a new phone number to the specified numbers in case the device is lost and then – block this device. You can unblock the device by entering the password set up to access the Anti-Theft module.

If it is necessary to change the password used to work with Anti-Theft module, select the **Change code** item. Enter the new password and its confirmation and press the **OK** button.

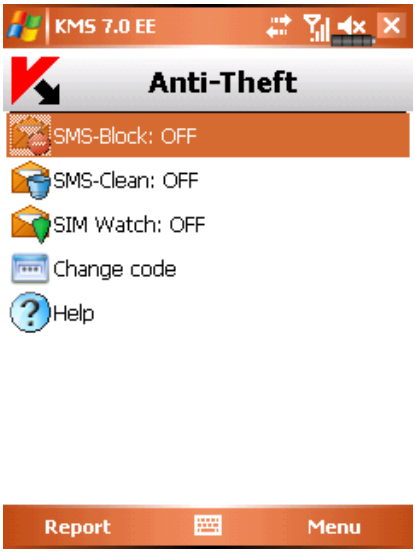

Figure 36. The **Anti-Theft** section

Information about the Anti-Theft module's work will be entered into the application log. To view the log, select the **Report** item in the **Anti-Theft** section.

The report is also available in the **Information** section (see section 3.8 on page 58);

3.4.2.1. SMS-Clean function's settings

The **SMS-Clean** function allows erasing date from the device if it gets lost (see Figure 37).

In order to change the SMS-Clean function settings, perform the following:

1. Open the **Anti-Theft** section
2. Enter the password and select **SMS-Clean** in the window that will open.
3. Check the **contacts** box if you wish the phone book to be deleted once your mobile device has been stolen or lost.
4. Check the **inbox** box if you wish to erase mail and SMS messages.
5. Check the **documents** box if you wish to erase user's personal files.
6. Check the **network settings** box if you wish to erase the network connection settings.
7. Check the **Files on the card** box if you wish to erase the files from the device memory card.
8. Press **Done** to save the changes.

Figure 37. SMS-Clean settings

3.4.2.2. SIM Watch function's settings

The **SIM Watch** function is designed to monitor replacement of the SIM card in the device (see Figure 38).

In order to change the SMS-Watch function settings, perform the following:

1. Open the **Anti-Theft** section
2. Enter the password and select **SIM Watch** in the window that will open.
3. Using fields **1)** and **2)** enter phone numbers to which you would like to receive a new phone number if the SIM card was replaced in your device. Such numbers may begin with a digit or with a "+" and must contain digits only.
4. Check the **Block** box to enable blocking of the device if its SIM card has been replaced.
5. Press **Done** to save the changes you have entered.

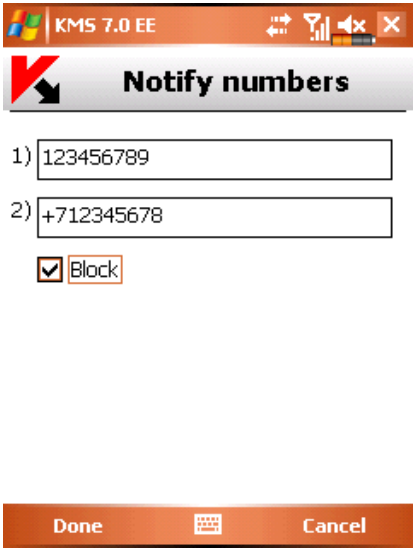

Figure 38. **SIM Watch** settings

3.5. Updating the application bases

Scan for malware programs is performed based on the records in the Kaspersky Mobile Security bases which contain description of all malware programs known at the moment. It is extremely important to keep you bases up-to-date.

You can update bases manually or according to a schedule. To configure and start the update use the **Update** tab (see Figure 39). Updates are performed from Kaspersky Lab's servers via internet.

Information about bases update will be entered into the log. In order to view the log select **Update report** in the **Update** section. The report is also available in the **Information** section (see section 3.8 on page 58);

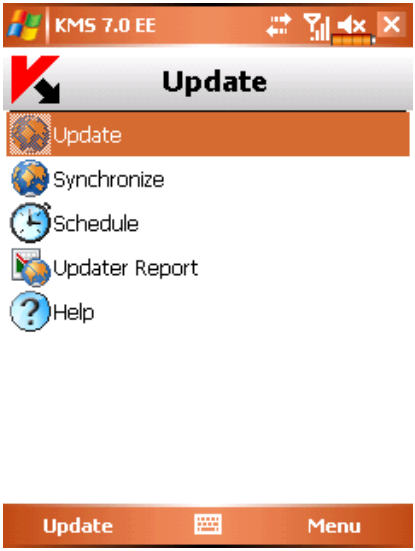

Figure 39. The **Update** section

In order to launch application bases updates manually, perform the following actions:

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 38) and open the **Update** section.
2. Select **Update** in order to start downloading updates.

To create an application bases update launch schedule, do the following.

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 38) and open the **Update** section.
2. Select the **Schedule** item.
3. Specify the update frequency in the **Automatic update** section:
   - **Daily** - the update to be launched every day. Additionally specify the **Time** of the update.
   - **Weekly** - the update will be launched once a week. Additionally specify the **Day of week** and the **Time** of the update.
   - **Manual** - the update will be manually launched by the user.

You can check the application base release date and the number of virus signatures it contains in the **Information** section. To do it, select the **About bases** item in this tab.

3.6. Updating the application operation settings

Note

For details about the joint operation of Kaspersky Mobile Security and Kaspersky Administration Kit see Kaspersky Mobile Security Administrator's Guide.

While using Kaspersky Mobile Security jointly with Kaspersky Administration Kit the application operation settings will be set by the policy for a group of mobile devices. Activation of the application and the applying of the policy settings blocked to prevent changes will take place when a device is being added to the administration group.

Later synchronization of the application with the Administration Server will be performed automatically using intervals set in the policy settings.

In order to start application manual synchronization with the Administration Server:

1. Start Kaspersky Mobile Security (see section 2.1.1 on page 9).
2. Open the **Update** section.
3. Select the **Synchronize** item.

During the synchronization the application operation settings will be loaded from the Administration Server and reports about the application's operation will be sent from the device to the application server. If the application operation settings did not change since the time of the last synchronization, the policy settings will not be applied.

3.7. Firewall

The **Firewall** module is designed for monitoring the network activity and protection of your mobile device at the network level (see Figure 40).

In order to change the Firewall settings, perform the following:

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 38) and open the **Firewall** section.
2. Select the **Firewall Settings** item. In the window that will open set the protection level to specify the level of monitoring of the incoming and outgoing traffic. You have the following options:

- **Block all** – any network activity except updating of bases and connection to Kaspersky Administration Kit is blocked.
- **Medium** – all incoming connections will be blocked, outgoing connections can only be established using SSH, HTTP, HTTPS, IMAP, SMTP ports.
- **Low** – only incoming connections are blocked.
- **Disabled** – all network activities are allowed.

Information about the operation of the Firewall will be entered into the log. In order to view the log, select **Update Report** in the **Update** section.

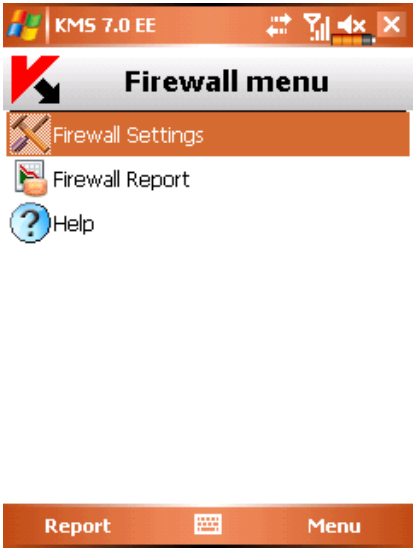

Figure 40. The **Firewall** section

3.8. Viewing reports about the application operation

Reports about the application's work are located in the **Reports** item of the **Information** tab. You can view a report on any task performed by Kaspersky Mobile Security:

- anti-virus scan;
- updating the application bases;

- firewall work;
- Anti-Spam module work;
- The Anti-Theft module work.

In order to view the report about the operation of one of the application components, do the following:

1. Start Kaspersky Mobile Security (see section 3.1.1 on page 38).
2. Select the **Reports** item in the **Information** tab (see Figure 41).
3. Select the report of the required component in the window that will open.

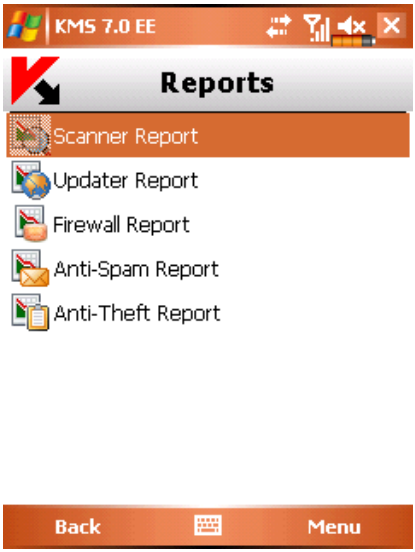

Figure 41. The **Reports** section

3.9. Uninstalling the application

In order to uninstall Kaspersky Mobile Security, perform the following actions:

1. Object protection mode (for details see section 3.2 on page 41);

Figure 42. Disabling Real-Time protection

2. Close Kaspersky Mobile Security. To do it, select the **Exit** menu item (see Figure 43).

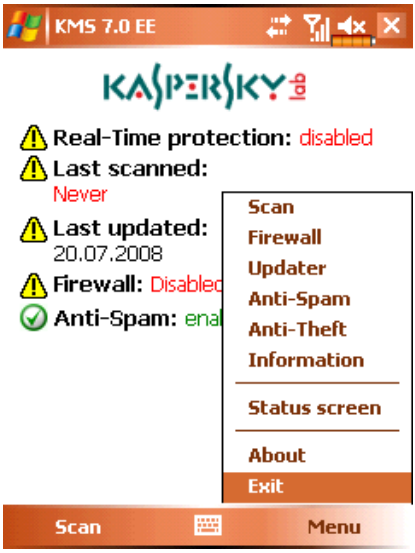

Figure 43. Closing the application

3. Uninstall the application. To do this:

   a) press the **Start** button, select the **Settings** menu, open the **System** tab and then switch to **Remove Programs** (see Figure 44):

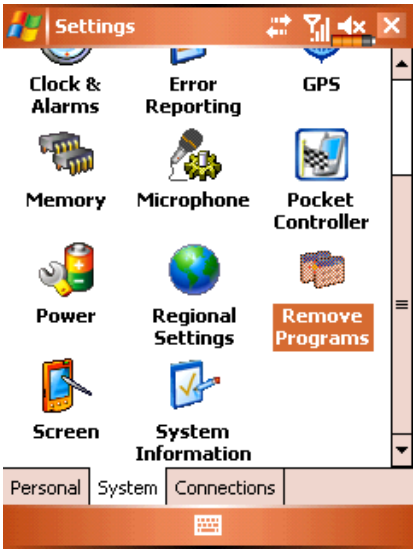

Figure 44. Starting removal of the application

   b) Select **Kaspersky Mobile Security** in the list of installed applications and press the **Remove** button (see Figure 45).

Figure 45. Selecting the application

c) Press the **Yes** button in the application removal confirmation window (see Figure 46). After this a notification about removal of file containing the application operation settings will open. Press **No** button in order to uninstall the entire application. If you press the **Yes** button, the fie with the application operation settings will preserved on the device.

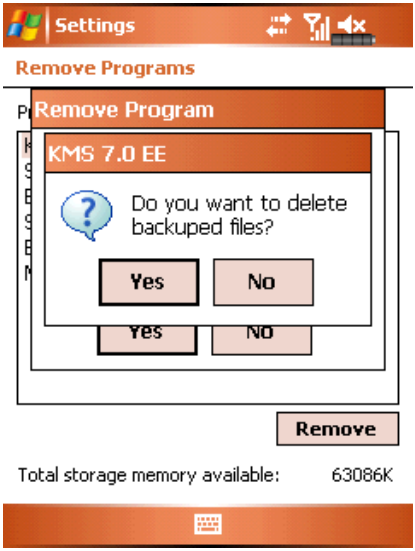

Figure 46. Prompt to save the application operation settings

APPENDIX A. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted email messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China, Poland, and Romania. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 450 specialists, each of whom is proficient in anti-virus technologies, with 10 of them holding M.B.A. degrees, 16 holding Ph.Ds, and senior experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company’s products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company’s flagship product, Kaspersky Internet Security, provides full-scale protection for all tiers of a network, including workstations, file servers, email systems, firewalls, Internet gateways, and hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Internet Security kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every hour. The company provides its customers with a 24-hour technical support service, which is available in several languages to accommodate its international clientele.

A.1. Other Kaspersky Lab Products

Kaspersky Lab News Agent

The News Agent is intended for timely delivery of news published by Kaspersky Lab, notifications about the current status of virus activity, and fresh news. The program reads the list of available news feeds and their content from the Kaspersky Lab news server at specified intervals.

News Agent enables users to;

- See the current virus forecast in the taskbar notification area
- Subscribe to and unsubscribe from news feeds
- Retrieve news from each selected feed at the specified interval and receive notifications about fresh news
- Review news on the selected feeds
- Review the list of feeds and their status
- Open full article text in your browser

News Agent is a stand-alone Microsoft Windows application that can be used independently or may be bundled with various integrated solutions offered by Kaspersky Lab.

Kaspersky® OnLine Scanner

This program is a free service provided to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer. Kaspersky OnLine Scanner runs directly from your browser. This way, users receive quick responses to questions regarding potential infectionson their computers. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning
- Select standard/extended databases for scanning
- Save a report on the scanning results in .txt or .html formats

Kaspersky® OnLine Scanner Pro

The program is a subscription service available to the visitors of Kaspersky Lab's corporate website. The service delivers an efficient online anti-virus scan of your computer and disinfects dangerous files. Kaspersky OnLine Scanner Pro runs directly from your browser. Using the service, visitors can:

- Exclude archives and e-mail databases from scanning
- Select standard/extended databases for scanning

- Save a report on the scanning results in .txt or .html formats

Kaspersky Anti-Virus® 7.0

Kaspersky Anti-Virus 7.0 is designed to safeguard personal computers against malicious software as an optimal combination of conventional methods of anti-virus protection and new proactive technologies.

The program provides for complex anti-virus checks, including:

- Anti-virus scanning of e-mail traffic on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used, as well as disinfection of e-mail databases.
- Real-time anti-virus scanning of Internet traffic transferred via HTTP.
- Anti-virus scanning of individual files, folders, or drives. In addition, a preset scan task can be used to initiate anti-virus analysis exclusively for critical areas of the operating system and start-up objects of Microsoft Windows.

Proactive protection offers the following features:

- *Controls modifications within the file system*. The program allows users to create a list of applications, which it will control on a per component basis. It helps protect application integrity against the influence of malicious software.
- *Monitors processes in random-access memory*. Kaspersky Anti-Virus 7.0 in a timely manner notifies users whenever it detects dangerous, suspicious or hidden processes or in case when unauthorized changes in active processes occur.
- *Monitors changes in OS registry* due to internal system registry control.
- *Hidden Processes Monitor* helps protect from malicious code concealed in the operating system using rootkit technologies.
- *Heuristic Analyzer.* When scanning a program, the analyzer emulates its execution and logs all suspicious activity, such as, opening or writing to a file, interrupt vector intercepts, etc. A decision is made based on this procedure regarding possible infection of the program with a virus. Emulation occurs in an isolated virtual environment which reliably protects the computer of infection.
- *Performs system restore* after malware attacks by logging all changes to the registry and computer file system and rolls them back at user's discretion.

Kaspersky® Internet Security 7.0

Kaspersky® Internet Security 7.0 is an integrated solution for protection of personal computers against the major information- threats (viruses, hackers, spam and spyware). A single interface enables fusers to configure and manage all the program's components.

The anti-virus protection features include:

- **Anti-virus scanning of e-mail traffic** on the level of data transmission protocol (POP3, IMAP and NNTP for incoming mail and SMTP for outgoing messages), regardless of the mail client being used. The program includes plug-ins for popular e-mail clients (such as Microsoft Office Outlook, Microsoft Outlook Express/Windows Mail, and The Bat!) and supports disinfection of their e-mail databases.
- **Real-time anti-virus scanning of Internet traffic** transferred via HTTP.
- **File system protection**: anti-virus scanning of individual files, folders or drives. In addition, the application can perform anti-virus analysis exclusively for critical areas of the operating system and Microsoft Windows start-up objects.
- **Proactive protection**: the program constantly monitors application activity and processes running in random-access memory, preventing dangerous changes to the file system and registry, and restores the system after malicious influence.

Protection against Internet-fraud is ensured by recognition of phishing attacks, thereby preventing confidential data leaks (above all passwords, bank account and credit card numbers) and blocking execution of dangerous scripts on web pages, pop-up windows and advertisement banners. The **autodialer blocking** feature helps identify software that attempts to use your modem for hidden unauthorized connections to paid phone services and blocks such activity.

Kaspersky Internet Security 7.0 **registers attempts to scan the ports of your computer**, which frequently precede network attacks, and successfully defends against typical network attacks. The program uses **defined rules as a basis** for control over all network transactions tracking all **incoming and outgoing data packets**. **Stealth Mode** (owing to the SmartStealth™ technology) **prevents computer detection from outside**. When you switch to Stealth Mode, the system blocks all network activity except for a few transactions allowed in user-defined rules.

The program employs an all-inclusive approach to anti-spam filtering of incoming e-mail messages:

- Verification against black and white lists of recipients (including addresses of phishing sites)
- Inspection of phrases in message body

- Analysis of message text using a learning algorithm
- Recognition of spam sent in image files

Kaspersky Anti-Virus for File Servers

This software package provides reliable protection for file systems on servers running Microsoft Windows, Novell NetWare, Linux and Samba from all types of malware. The suite includes the following Kaspersky Lab applications:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Windows Server.
- Kaspersky Anti-Virus for Linux File Server.
- Kaspersky Anti-Virus for Novell Netware.
- Kaspersky Anti-Virus for Samba Server.

Features and functionality:

- *Protects server file systems in real time*: All server files are scanned when opened or saved on the server
- *Prevents virus outbreaks;*
- *On-demand scans* of the entire file system or individual files and folders;
- *Use of optimization technologies* when scanning objects in the server file system;
- *System rollback after virus attacks;*
- *Scalability of the software package* within the scope of system resources available;
- *Monitoring of the system load balance;*
- *Creating a list of trusted processes* whose activity on the server is not subject to control by the software package;
- *Remote administration* of the software package, including centralized installation, configuration, and administration;
- *Saving backup copies of infected and deleted objects* in case you need to restore them;
- *Quarantining suspicious objects;*
- *Send notifications on events* in program operation to the system administrator;
- *Log detailed reports;*

- *Automatically update program databases.*

Kaspersky Open Space Security

Kaspersky Open Space Security is a software package withal new approach to security for today's corporate networks of any size, providing centralized protection information systems and support for remote offices and mobile users.

The suite includes four programs:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Specifics on each program are given below.

Kaspersky WorkSpace Security is a program for centralized protection of workstations inside and outside of corporate networks from all of today's Internet threats (viruses, spyware, hacker attacks, and spam).

Features and functionality:

- Comprehensive protection from viruses, spyware, hacker attacks, and spam;
- Proactive Defense from new malicious programs whose signatures are not yet added to the database;
- Personal Firewall with intrusion detection system and network attack warnings;
- Rollback for malicious system modifications;
- Protection from phishing attacks and junk mail;
- Dynamic resource redistribution during complete system scans;
- Remote administration of the software package, including centralized installation, configuration, and administration;
- Support for Cisco® NAC (Network Admission Control);
- Scanning of e-mail and Internet traffic in real time;
- Blocking of popup windows and banner ads when on the Internet;
- Secure operation in any type of network, including Wi-Fi;
- Rescue disk creation tools that enable you to restore your system after a virus outbreak;

- An extensive reporting system on protection status;
- Automatic database updates;
- Full support for 64-bit operating systems;
- Optimization of program performance on laptops (Intel® Centrino® Duo technology);
- Remote disinfection capability (Intel® Active Management, Intel® vPro™).

Kaspersky Business Space Security provides optimal protection of your company's information resources from today's Internet threats. Kaspersky Business Space Security protects workstations and file servers from all types of viruses, Trojans, and worms, prevents virus outbreaks, and secures information while providing instant access to network resources for users.

Features and functionality:

- Remote administration of the software package, including centralized installation, configuration, and administration;
- Support for Cisco® NAC (Network Admission Control);
- Protection of workstations and file servers from all types of Internet threats;
- iSwift technology to avoid rescanning files within the network;
- Distribution of load among server processors;
- Quarantining suspicious objects from workstations;
- Rollback for malicious system modifications;
- scalability of the software package within the scope of system resources available;
- Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database;
- Scanning of e-mail and Internet traffic in real time;
- Personal Firewall with intrusion detection system and network attack warnings;
- Protection while using Wi-Fi networks;
- Self-Defense from malicious programs;
- Quarantining suspicious objects;
- automatic database updates.

Kaspersky Enterprise Space Security

This program includes components for protecting linked workstations and servers from all today's Internet threats. It deletes viruses from e-mail, keeping information safe while providing secure access to network resources for users.

Features and functionality:

- Protection of workstations and file servers from viruses, Trojans, and worms;
- Protection of Sendmail, Qmail, Postfix and Exim mail servers;
- Scanning of all e-mails on Microsoft Exchange Server, including shared folders;
- Processing of e-mails, databases, and other objects for Lotus Domino servers;
- Protection from phishing attacks and junk mail;
- preventing mass mailings and virus outbreaks;
- scalability of the software package within the scope of system resources available ;
- Remote administration of the software package, including centralized installation, configuration, and administration;
- Support for Cisco ® NAC (Network Admission Control);
- Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;
- Personal Firewall with intrusion detection system and network attack warnings ;
- Secure operation while using Wi-Fi networks;
- Scans Internet traffic in real time;
- Rollback for malicious system modifications;
- Dynamic resource redistribution during complete system scans;
- Quarantining suspicious objects ;
- An extensive reporting system on protection system status;
- automatic database updates.

Kaspersky Total Space Security

This solution monitors all inbound and outbound data streams (e-mail, Internet, and all network interactions). It includes components for protecting workstations and mobile devices, keeps information safe while providing secure access for users to the company's information resources and the Internet, and ensures secure e-mail communications.

Features and functionality:

- Comprehensive protection from viruses, spyware, hacker attacks, and spam on all levels of the corporate network, from workstations to Internet gateways;
- Proactive Defense for workstations from new malicious programs whose signatures are not yet added to the database ;
- Protection of mail servers and linked servers;
- Scans Internet traffic (HTTP/FTP) entering the local area network in real time;
- scalability of the software package within the scope of system resources available ;
- Blocking access from infected workstations;
- Prevents virus outbreaks;
- Centralized reporting on protection status;
- Remote administration of the software package, including centralized installation, configuration, and administration;
- Support for Cisco® NAC (Network Admission Control);
- Support for hardware proxy servers;
- Filters Internet traffic using a trusted server list, object types, and user groups;
- iSwift technology to avoid rescanning files within the network ;
- Dynamic resource redistribution during complete system scans;
- Personal Firewall with intrusion detection system and network attack warnings ;
- Secure operation for users on any type of network, including Wi-Fi;
- Protection from phishing attacks and junk mail;
- Remote disinfection capability (Intel® Active Management, Intel® vPro™);

- Rollback for malicious system modifications;
- Self-Defense from malicious programs;
- full support for 64-bit operating systems;
- automatic database updates.

Kaspersky Security for Mail Servers

This program is for protecting mail servers and linked servers from malicious programs and spam. The program includes application for protecting all standard mail servers (Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix and Exim) and also enables you to configure a dedicated e-mail gateway. The solution includes:

- Kaspersky Administration Kit.
- Kaspersky Mail Gateway.
- Kaspersky Anti-Virus for Lotus Notes/Domino.
- Kaspersky Anti-Virus for Microsoft Exchange.
- Kaspersky Anti-Virus for Linux Mail Server.

Its features include:

- Reliable protection from malicious or potentially dangerous programs;
- Junk mail filtering;
- Scans incoming and outgoing e-mails and attachments;
- Scans all e-mails on Microsoft Exchange Server for viruses, including shared folders;
- Processes e-mails, databases, and other objects for Lotus Notes/Domino servers;
- Filters e-mails by attachment type;
- Quarantines suspicious objects;
- Easy-to-use administration system for the program;
- Prevents virus outbreaks;
- Monitors protection system status using notifications;
- Reporting system for program operation;
- scalability of the software package within the scope of system resources available ;

- automatic database updates.

Kaspersky Security for Internet Gateways

This program provides secure access to the Internet for all an organization's employees, automatically deleting malware and riskware from the data incoming on HTTP/FTP. The solution includes:

- Kaspersky Administration Kit.
- Kaspersky Anti-Virus for Proxy Server.
- Kaspersky Anti-Virus for Microsoft ISA Server.
- Kaspersky Anti-Virus for Check Point FireWall-1.

Its features include:

- Reliable protection from malicious or potentially dangerous programs;
- Scans Internet traffic (HTTP/FTP) in real time;
- Filters Internet traffic using a trusted server list, object types, and user groups;
- Quarantines suspicious objects;
- Easy-to-use administration system;
- Reporting system for program operation;
- Support for hardware proxy servers;
- Scalability of the software package within the scope of system resources available ;
- Automatic database updates.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite designed to help organizations with small- and medium-sized networks wage war against the onslaught of unsolicited e-mail messages (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including DNS Black Lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database, adding samples provided by the Company's linguistic laboratory specialists. Databases are updated every 20 minutes.

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper provides high-speed scanning of traffic on servers running Clearswift MIMEsweeper for SMTP / Clearswift MIMEsweeper for Exchange / Clearswift MIMEsweeper for Web.

The program is a plug-in and scans for viruses and processes inbound and outbound e-mail traffic in **real** time.

A.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our **product** by phone or via email. Rest assured that all of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html Helpdesk: www.kaspersky.com/helpdesk.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com E-mail: info@kaspersky.com

APPENDIX B. LICENSE AGREEMENT

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (“AGREEMENT”), FOR THE LICENSE OF KASPERSKY MOBILE SECURITY ENTERPRISE EDITION (“SOFTWARE”) PRODUCED BY KASPERSKY LAB (“KASPERSKY LAB”).

IF YOU HAVE PURCHASED THIS SOFTWARE VIA THE INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD/DVD’S SLEEVE YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD/DVD’s SLEEVE, DOWNLOAD, INSTALL OR USE THIS SOFTWARE.

IN ACCORDANCE WITH THE LEGISLATION, REGARDING KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS PURCHASED ONLINE FROM THE KASPERSKY LAB OR ITS PARTNER’S INTERNET WEB SITE, CUSTOMER SHALL HAVE A PERIOD OF FOURTEEN (14) WORKING DAYS AS FROM THE DELIVERY OF PRODUCT TO MAKE RETURN OF IT TO THE MERCHANT FOR EXCHANGE OR REFUND, PROVIDED THE SOFTWARE IS NOT UNSEALED.

REGARDING THE KASPERSKY SOFTWARE INTENDED FOR INDIVIDUAL CONSUMERS NOT PURCHASED ONLINE VIA INTERNET, THIS SOFTWARE NEITHER WILL BE RETURNED NOR EXCHANGED EXCEPT FOR CONTRARY PROVISIONS FROM THE PARTNER WHO SELLS THE PRODUCT. IN THIS CASE, KASPERSKY LAB WILL NOT BE HELD BY THE PARTNER'S CLAUSES.

THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to “Software” herein shall be deemed to include the software activation code with which you will be provided by Kaspersky Lab as part of the Kaspersky Mobile Security 7.0 Enterprise Edition.

1. *License Grant*. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants you the non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one device.

1.1 *Use*. The Software is licensed as a single product; it may not be used on more than one device or by more than one user at a time, except as set forth in this Section.

1.1.1 The Software is "in use" on a device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD/DVD-ROM, or other storage device) of that device. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You shall maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

1.1.2 The Software protects device against viruses and network attacks whose signatures are contained in the threat signatures and network attacks databases which are available on Kaspersky Lab's update servers.

1.1.3 If you sell the device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

1.1.4 You shall not decompile, reverse engineer, disassemble or otherwise reduce any part of this Software to a humanly readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created programs will be provided by Kaspersky Lab by request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event that Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability, provided that you only reverse engineer or decompile the Software to the extent permitted by law.

1.1.5 You shall not make error corrections to, or otherwise modify, adapt, or translate the Software, nor create derivative works of the Software, nor permit any third party to copy (other than as expressly permitted herein).

1.1.6 You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

1.1.7 You shall not provide the activation code or license key file to third parties or allow third parties access to the activation code or license key. The activation code and license key are confidential data.

1.1.8 Kaspersky Lab may ask User to install the latest version of the Software (the latest version and the latest maintenance pack).

1.1.9 You shall not use this Software in automatic, semi-automatic or manual tools designed to create virus signatures, virus detection routines, any other data or code for detecting malicious code or data.

2. *Support*.

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period, specified in the License Key File and indicated in the "Service" window, since the moment of activation on:

(a) payment of its then current support charge, and:

(b) successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab website, which will require you to enter activation code which will have been provided to you by Kaspersky Lab with this Agreement. It shall be at the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

Support Services shall become available after Software activation. Kaspersky Lab's technical support service is also entitled to demand from the End User additional registration for identifier awarding for Support Services rendering.

Until Software activation and/or obtaining of the End User identifier (Customer ID) technical support service renders only assistance in Software activation and registration of the End User.

(ii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy, which is deposited on www.kaspersky.com/privacy, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iii) Support Services will terminate unless renewed annually by payment of the then-current annual support charge and by successful completion of the Support Services Subscription Form again.

(iv) "Support Services" means:

(a) Hourly updates of the anti-virus database;

(b) Updates of network attacks database;

(c) Updates of anti-spam database;

(d) Free software updates, including version upgrades;

(e) Technical support via Internet and hot phone-line provided by Vendor and/or Reseller;

(f)Virus detection and disinfection updates in 24-hours period.

(v) Support Services are provided only if and when you have the latest version of the Software (including maintenance packs) as available on the official Kaspersky Lab website (www.kaspersky.com) installed on your device.

3. *Ownership Rights*. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all rights, titles and interests in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer any title to the intellectual property in the Software to you, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

4. *Confidentiality*. You agree that the Software and the Documentation, including the specific design and structure of individual programs constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide, or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavors to maintain the security of the activation code.

5. *Limited Warranty*.

(i) Kaspersky Lab warrants that for six (6) months from first download or installation the Software purchased on a physical medium will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

(ii) You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted or error free.

(iii) Kaspersky Lab does not warrant that this Software identifies all known viruses and spam letters, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus.

(iv) Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item.

(v) The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended, or (c) use the Software other than as permitted under this Agreement.

(vi) The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (vi) have effect between the Kaspersky Lab and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

6. *Limitation of Liability*.

(i) Nothing in this Agreement shall exclude or limit Kaspersky Lab's liability for (a) the tort of deceit, (b) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, or (c) any other liability which cannot be excluded by law.

(ii) Subject to paragraph (i) above, Kaspersky Lab shall bear no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

(a) Loss of revenue;

(b) Loss of actual or anticipated profits (including for loss of profits on contracts);

(c) Loss of the use of money;

(d) Loss of anticipated savings;

(e) Loss of business;

(f) Loss of opportunity;

(g) Loss of goodwill;

(h) Loss of reputation;

(i) Loss of, damage to or corruption of data, or:

(j) Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraphs (ii), (a) to (ii), (i).

(iii) Subject to paragraph (i), the liability of Kaspersky Lab (whether in contract, tort, restitution or otherwise) arising out of or in connection with

the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

7. This Agreement contains the entire understanding between the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date.

When using demo software, you are not entitled to the Technical Support specified in Clause 2 of this EULA, nor do you have the right to sell the copy in your possession to other parties.

You are entitled to use the software for demo purposes for the period of time specified in the license key file starting from the moment of activation (this period can be viewed in the Service window of the software's GUI).